CTC 456 – Enterprise System Security
Spring 2023

Instructor	Fnu Saurabh	**E-Mail**	slnu3@csudh.edu
Classroom	SAC 2102	**Class Time**	Tu Th 5:30pm-6:45pm
Office	Online	**Office Hours**	Online by appointment
Phone		**URL**	http://csc.csudh.edu

CATALOG DESCRIPTION:

This course teaches students through lectures, discussions, demonstrations, and classroom labs. Students learn the knowledge, skills, and abilities necessary to identify and fix network vulnerabilities using penetration testing techniques. This course is intended for people interested in security operations and cybersecurity roles.

TEXTBOOK

MITRE ATT&CK: Design and Philosophy MITRE ATT&CK is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. **– Students can download the ebook at the given link below.**
https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

Cybersecurity Incident & Vulnerability Response Playbooks - Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems - This playbook provides a standardized response process for cybersecurity incidents and describes the process and completion through the incident response phases as defined in National Institute of Standards and Technology (NIST) Special Publication
https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

REFERENCE*:*

TBA

COURSE GOALS:

The primary objective of this course is to introduce students to the NIST Cybersecurity Framework and expose them, via practical hands-on exercises, to common security controls and solutions used in an enterprise level security operations center or a network operations center.

The primary objective of this course is to teach students the necessary skills for a security operations center to determine the feasibility of a particular set of attack vectors, identifying higher-risk vulnerabilities, and responding to various types of cyber threats and identifying vulnerabilities that may be difficult or impossible to detect with automated network or application vulnerability scanning software. The course presents the process in developing enterprise level operational security skills using existing tools, techniques, and programming languages. Our mission is to teach individuals the essential skills and techniques needed to protect and secure an organization's critical information assets and business systems.

COURSE OUTCOMES:

Upon completion of this course, students will be able to:

- Identify, enumerate, and mitigate vulnerable systems
- Understand the working of enterprise level security operations.
- Patch application-level holes and defenses
- Understand advanced controls that can be deployed to protect network infrastructure.
- Understand the essential incident handling and forensics methodology.
- Understand advanced controls that can be deployed to protect network infrastructure. Understand the essential incident handling and forensics methodology.
- Identifying and removing malware
- Demonstrate an understanding of how to manage risk, threats, and vulnerabilities.
- Utilize port scanners and discovery tools
- Understand penetration testing methodologies
- Perform network reconnaissance
- Using Automated tools to find network security vulnerabilities
- Demonstrate an understanding of how to manage risk, threats, and vulnerabilities.
- An understanding of the severity and types of insider threats and how to protect against them.
- Understand risks and vectors associated with confidential data leakage and be able to implement best practices to detect and prevent data loss.
- Understand the characteristics and capabilities of rootkits and bootkits as well as tools that can be used for detection and removal.
- Understanding of fundamental information security and risk management concepts.
- Demonstrate an understanding of access controls and effective authentication, authorization, and accountability.
- Demonstrate a fundamental understanding of cryptographic algorithms and how cryptography is used to protect information and communications.
- Demonstrate an understanding of securing networks from common attacks against wired, wireless, VoIP, virtual and cloud-based network services.
- Understand a command and control system (C2) and adversary's tools techniques and procedures in order to protect the environment.
- Demonstrate the ability to create, harden, and maintain a medium sized business system.

COMPUTER INFORMATION LITERACY EXPECTATIONS

It is expected that students will:

1. *Use Microsoft Word for word processing unless otherwise approved by the instructor.*
2. *Be familiar with using email as a communication tool and check your official campus email account at least every other day.*
3. *Be able to access websites and online course materials which may require Flash and other plug-ins.*
4. *Use the library databases to find articles, journals, books, databases and other materials.*
5. *Be able to create an effective PowerPoint presentation.*
6. *Be able to record audio (ideally video) to share with the instructor via the web.*
7. *Have regular access to a computer and internet access for the term of this course.*

TECHNOLOGY REQUIREMENTS

Computer:

You must have access to a reliable computer for this course. If you are on campus, and do not have a laptop, you can check out a laptop from the IT User Services Help Desk via Technology Checkout Program. In addition, the CSUDH Toro Lab offers on campus access to workstations with a wide variety of commonly used software.

Visit the CSUDH Academic Technology Online Courses Technical Requirements page for more information on technology requirements.

Email:

All email communications from this course will go through your Toromail. Toromail is the CSUDH student email system.

Internet and Campus Wireless Network:

You must have Internet access to participate in this course. If you are on campus, connect your laptop and mobile device to the internet using the eduroam campus wireless network.

Office 365:

Course work will require you to submit work in Word format (.docx files). Active CSUDH students have access to Office 365 (Word, Excel, PowerPoint) for personal desktop and laptop computers at no cost.

ATTENDANCE:

Students are expected and encouraged to attend lectures and contribute to discussions. It is thestudent's responsibility to contact the instructor as early as possible if he/she cannot attend class. Therewill be no make-up opportunities, although all classes will have companion videos available online.

The student is responsible for materials missed during an absence, whether excused or not. Classes will start at the prescribed time and will end at the prescribed time. Instructor will be available during the posted office hours, and you may make an appointment for times not posted.

GRADING BREAKDOWN:

Mid Terms	25%
Finals	35%
Assignments & Labs	40%
	100%

Evaluation criteria explained:

- Students are expected to be active participants in each class meeting. Full credit for participation will be extended to students who regularly ask questions, share observations, and contribute relevant personal experiences.
- The mid-term examination will consist of objective questions and will require a technological comprehension that covers the lecture material and assigned readings.
  The assignments will consist of several in class and homework tasks.
- Students will be given specific guidance on the amount of collaboration permitted for each assignment. Unless otherwise specified, all assignments are individual assignments, and thus must be completely the original work of the student submitting them and include proper citations to the published work of others.

Quizzes:

Quizzes may be given throughout the semester, at a rate of approximately 1 per week. Quizzes will always cover the material covered since the last Quiz or Exam. The quizzes will be combinations of objective and short-answer questions. Quizzes will be administered online via Blackboard. Makeup quizzes will not be given. However, the lowest quiz grade will be dropped. Any class material missed by the student is the student's responsibility to acquire.

MIDTERM & FINAL EXAM:

Midterm exam is during the 8th week of the class and the date for the final exam is based on the final examination schedule printed in the campus Class Schedule. All projects are due no later than the last week of the semester.

No makeup or early exams will be administered except in cases outlines in course policy.

GRADES:

The following grading scale will be used:

Score	Grade	Score	Grade
96-100	A	90-95	A-
87-89	B+	83-86	B
80-82	B-	77-79	C+
73-76	C	70-72	C-
67-69	D+	63-66	D
0-62	F		

COURSE POLICIES:

- Deliverables (Class Assignments, Projects) are due before the last day of class each week based on the course schedule.
- Deliverables (Class Assignments, Projects) submitted late are not accepted.
- Deliverables (Class Assignment, Projects) not submitted before the end of the final class will earn 0%.
- Any exceptional, non-academic circumstances need to be discussed with the instructor as soon as they arise, prior to the due date of the deliverable or exam. At the time of the discussion, NO make-up work will be assigned.
- The instructor reserves the right not to award credit for deliverables that are incomplete. Partial credit is awarded at the instructor's discretion, and only for work that merits such an award. Assignments that are incomplete or incongruous with the specifications may be returned to the student.
- Extra credit assignments will be made available to all students. Extra credit will be applied to the final exam and will not exceed 10 percent.

GENERAL POLICIES:

ACADEMIC HONOR CODE

Programming assignments must be done individually. Failure to do so will result in a violation of the CSUDH Academic Honor Code. The following cases will be considered as violations: identical code, and extremely similar code. Violations will be reported to the Office of Vice President of Academic Affairs. Disciplinary action will be taken against any student who alone or with others engages in any act of academic fraud or deceit (Read University Regulations in University Catalog). It is the student's responsibility to ensure they fully understand to what extent they may collaborate or discuss content with other students. No exam work may be performed with the assistance of others or outside material unless specifically instructed as permissible. If an exam or assignment is designated "no outside assistance" this includes, but is not limited to, peers, books, publications, the Internet and the WWW. If a student is instructed to provide citations for sources, proper use of citation support is expected.

ATTENDANCE POLICY

Excessive absences will result in lowered grades. Excessive absenteeism, whether excused or unexcused, may result in a student's course grade being reduced or in assignment of a grade of "F". Absences areaccumulated beginning with the first day of class.

STUDENT ACADEMIC APPEALS PROCESS

Authority and responsibility for assigning grades to students' rests with the faculty. However, in those instances where students believe that miscommunication, error, or unfairness of any kind may have adversely affected the instructor's assessment of their academic performance, the student has a right to appeal by the procedure listed in the Undergraduate Catalog and by doing so within thirty days of receiving the grade or experiencing any other problematic academic event that prompted the complaint.

ADA STATEMENT

Students with disabilities, who believe they may need an academic adjustment in this class, are encouraged to contact me as soon as possible to better ensure receipt of timely adjustments.

TECHNICAL HELP

If you need technical help, refer to the following resources:

Login Issues:

For login issues related to Blackboard, Toromail and MyCSUDH, contact the IT Help Desk at (310) 243-2500, option 1. You can also create an online service ticket for login support.

The IT Help Desk also offers walk-in support. Visit the first floor of the library (north), C-108, for in-person help.

Password Resets:

CSUDH offers an easy, self-service password reset service at https://password.csudh.edu/. For additional assistance with password resets, contact the IT Help Desk.

Blackboard Issues:

For issues or questions with Blackboard, contact the CSUDH Blackboard Support line at (310) 243-2500, option 2. You can also create an online service ticket for Blackboard support.

Need Help with Using Blackboard?

If you are new to Blackboard or unfamiliar with a specific feature of Blackboard, CSUDH Academic Technology offers a series of PDF and video-based tutorials. Visit the CSUDH Academic Technology Tutorials page for more information.

Instructor's Rights

An instructor has the right to remove a student from class at any time he/she considers a student's actions to be interfering with a proper collegiate environment. The instructor may also refer the incident to the Director of Student Discipline & Student Life for disciplinary action as warranted.

TENTATIVE COURSE OUTLINE

(Will be conducted according to the following. However, the schedule of the topics schedule or timetable may be varying slightly)

Week #	***Date***	***Topic***	***Reading Assignment/ Computer Lab Topic/In Class Assignments***
Week 1	24-Jan	Or-view, Introduction, and terminologies	Assignment/Lab – 1
Week 2	31-Jan	Virtualization, Linux and containers	
Week 3	7-Feb	security operations center and Indicator of compromise	Assignment/Lab – 2
Week 4	14-Feb	MITRE ATT&CK, Cyber Kill chain	Assignment/Lab – 3
Week 5	21-Feb	Incident Response and IR life cycle	Assignment/Lab – 4
Week 6	28-Feb	Vulnerability Management, Firewall, IDS and IPS	
Week 7	7-Mar	Log based hunting, SIEM	Assignment/Lab – 5
Week 8	14-Mar	Hunting with Splunk	
Week 9	21-Mar	Identity and Access Management (IAM), Authentication, SSO & MFA	Assignment/Lab – 6
Week 10	4-Apr	Endpoint security, AV, Sandbox	Assignment/Lab – 7
Week 11	11-Apr	Threat Intelligence and intel led security	
Week 12	18-Apr	Career prospects and blue teaming jobs	Assignment/Lab – 8
Week 13	25-Apr	Threat Modeling Security architecture	Assignment/Lab – 9
Week 14	2-May	Creating a security policy for enterprise systems	Assignment/Lab – 10
Week 15	9-May	**EXAM**	